



088865

088865

IMPROVING GENERALISTS' CAPABILITIES

IN ASSESSING OUTPUT RELIABILITY

AND INTERNAL CONTROLS

IN COMPUTER-BASED SYSTEMS

U.S. GENERAL ACCOUNTING OFFICE

DENVER REGIONAL OFFICE

2420 WEST 26th AVENUE, SUITE 300-D

DENVER, COLORADO 80211

NOVEMBER 1982

CONTACTS:

Robert W. Hanlon, Regional Manager  
Arley R. Whitsell, Assistant Regional Manager  
Norman G. Austen, ADP Specialist  
Pamela K. Tumbler, Writer-Editor

(303) 837-4621  
FTS 327-4621

730159

## EXECUTIVE SUMMARY

The public and private sectors increasingly rely on computerized systems to collect, process, store and distribute data. Thus, it is imperative that GAO's computer-related audit competencies keep pace with the rapidly increasing advances in, and use of, electronic technology.

GAO's "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions" requires evaluators to review internal (general and application) controls of computer-based systems involved in our reviews. GAO policy, recognizing that compliance with this requirement is not always feasible, places responsibility on the evaluator for performing, at a minimum, enough audit work to assess the reliability of any computer-generated information which will be used in support of audit findings or could otherwise affect the audit results. While it is sometimes infeasible to review a computer-based system's internal controls, at other times it is unnecessary. Just as the necessity and feasibility of reviewing internal controls will vary according to the assignment, so too will the type and extent of audit work needed to review internal controls or to assess computer output reliability. By gathering and analyzing information on a computer-based system, the type and extent of audit work needed--not only on the current job, but also as a separate assignment--can be determined, thus enabling cost-effective application of our computer-related audit resources.

However, a recent Denver Regional Office study indicates that not enough information is gathered on computer-based systems to allow such determinations to be made. Among the factors which contribute to the lack of adequate data gathering on computer-based systems are the following:

- Most of our generalist evaluators have little ADP knowledge and computer-related audit experience.
- The two GAO audit guides intended for generalists' guidance in assessing computer output reliability and evaluating internal controls are too complex for most generalists, and take considerable time to use (about 30 and 180 staff days, respectively, for a simple computer-based system).

Over the long term, our generalists' computer-related audit skills need to be improved through extensive training and on-the-job experience. In the meantime, an approach is needed whereby we can assure that (1) sufficient data is gathered, in a timely manner, on computer-based systems involved in our reviews; (2) the appropriate type and extent of computer-related audit work needed on a job is determined, performed, and documented; and (3) our computer-related audit resources are applied cost-effectively on both current and future jobs.

The Denver Regional Office has developed, tested, and refined such an approach. This approach consists of

- a one-page computer data collection instrument (DCI) which can be administered by a generalist in about 5 staff-days and
- a decisionmaking process which can assist managers in applying their computer-related audit resources effectively and economically.

## GLOSSARY

### Application controls

Controls which relate to a computer's processing functions. The purpose of such controls is to assure that data are processed in a timely, accurate, and complete manner. While they may be unique to a particular application, these controls can generally be grouped according to the following stages of processing:

- Data organization.

- Data input.

- Data processing.

- Data output.

### Computer-based system

Not merely a computer, but a number of elements, each of which performs a function in the system. Basically, a computer-based system is comprised of

- an electronic data processor (central processing unit);

- peripheral equipment (data preparation, input, and output devices);

- procedures that describe what data are needed, when and how they are obtained, and what their ultimate uses are;

- instruction routines for the processor; and

- personnel to operate and maintain equipment, establish and analyze procedures, prepare instructions, provide input data, distribute and use reports, review results, and supervise the system's operation.

Computer-based systems are generally categorized as either simple or complex. A simple system has one set of data inputs, one processor, and one set of outputs. A complex system has many data bases, possibly several central processors, and various outputs. Additionally, a complex system may be internettted to another computer system.

### General controls

Controls which relate to all activities of an organization with a computer-based information system. General controls include

- organizational controls;

- administrative controls;

- system design, development, and verification controls;

- data center management and protection controls; and

- system software controls and hardware controls.

IMPROVING GENERALISTS' CAPABILITIES IN  
ASSESSING OUTPUT RELIABILITY AND INTERNAL  
CONTROLS IN COMPUTER-BASED SYSTEMS

GAO's "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions" requires assessment of internal (general and application) controls in computer-based systems involved in our reviews:

"\* \* \* (T)he auditors shall:

- a. Review general controls in data processing systems to determine whether (1) the controls have been designed according to management direction and known legal requirements, and (2) the controls are operating effectively to provide reliability of, and security over, the data being processed.
- b. Review application controls of installed data processing applications upon which the auditor is relying to assess their reliability in processing data in a timely, accurate, and complete manner."

According to GAO policy, when compliance with these standards is not feasible, the evaluator is still responsible for performing sufficient evaluation work to provide reasonable assurance that any computer-processed information used in a GAO review is relevant, accurate, and complete, consistent with its intended use.

OBJECTIVE, SCOPE, AND METHODOLOGY

The Denver Regional Office recently conducted a study to determine how it can most efficiently and effectively meet GAO audit standards and policy for reviews involving computer-based systems. We interviewed Denver evaluators assigned to 35 reviews being conducted in the region. We also reviewed numerous directives and statements on applying auditing principles to computer-based systems. Among those reviewed were

- The American Institute of Certified Public Accountants' "Statements on Auditing Standards" numbers 1, 3, and 30;
- The Canadian Institute of Chartered Accountants' "Computer Control Guidelines" and "Computer Audit Guidelines;" and
- GAO's "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions;" "Assessing Reliability of Computer Output;" "Evaluating Internal Controls in Computer-Based Systems;" "General Policy Manual;" "Project Manual;" and "Policy and Procedures Manual for Guidance of Federal Agencies (Title 2 - Accounting)."

Although our observations apply only to Denver staff, we believe that many of them are equally applicable to GAO staff in general.

Throughout this report, we use the following terms to describe our audit staff:

- Generalist evaluators, who comprise the majority of our staff, are those who have little or no ADP knowledge or expertise.
- Generalist evaluators with ADP expertise are those who have considerable ADP knowledge and experience.
- Technical Assistance Group (TAG) specialists, who are limited in number, are those who provide technical advice and special assistance on reviews involving computer-based systems.

Other audit organizations similarly classify their audit staff. For example, the Australian Auditor General's Office classifies its audit staff as either generalists (those who have completed basic courses in ADP), advanced generalists (those who have completed basic courses and have experience in auditing computer-based systems), or ADP branch staff (those who have considerable ADP expertise and experience).

Although we believe that throughout the coming years GAO's generalist evaluators will need extensive training to effectively meet the increasing challenges of auditing in a computer environment, we did not address computer-related training needs in this study. Rather, we focused on developing a more immediate solution--an approach by which we can improve our computer-related audit efforts within our current resources and staff capabilities.

#### DATA GATHERING IS THE KEY TO COMPUTER-RELATED AUDIT WORK

Despite the audit standards' implications to the contrary, GAO policy recognizes that it is not always necessary or feasible to review internal controls and assess computer output reliability on reviews involving computer-based systems. Rather, the type and extent of computer-related audit work deemed necessary or feasible varies according to the assignment. Before considerable resources are expended to assess either computer output reliability or internal controls, it is vital that the assessment be determined necessary, appropriate, and cost-effective. Until sufficient information has been gathered on a computer-based system, however, the type and extent of related audit work needed on a particular assignment cannot be determined. Therefore, on every review involving a computer-based system, sufficient data must be gathered to allow such a determination to be made.

#### When must computer output reliability and internal controls be assessed?

Although GAO audit standards state that on every job involving a computer-based system, both internal controls and output reliability must be assessed, either or both assessments may be unnecessary or infeasible. For example, an internal control review may not be necessary if the computer-based system in question has recently been reviewed by GAO, another audit group, or the agency (in accordance with OMB Circular A-123). Similarly, an output reliability assessment may not be necessary if the data to be used to support audit findings are not computer generated.

Various factors dictate the feasibility of assessing either internal controls or output reliability. Time, for example, is often a critical factor. The time required to assess a system's internal controls as a part of the job may exceed the time required to complete the entire job. Other factors, such as the availability of source data and the significance of computer manipulation of data, may render reliability assessment infeasible.

Of course, computer output reliability assessments and internal control reviews are often necessary. For example, when computer output will be used to support audit findings or will otherwise affect the review results, the reliability of that data must be assessed. Similarly, a computer-based system's internal controls must be reviewed to provide a basis for reliance on them or to determine the scope of work necessary in financial audits.

Just as the need for an assessment of computer output reliability or internal controls varies according to the assignment, so too does the type and amount of work necessary to complete the assessment. A full-scale internal control review or a detailed output reliability assessment may be necessary on some assignments; on other assignments, a few simple tests may suffice.

### How are output reliability and internal controls assessed?

GAO has published two audit guides to assist its staff in performing work involving computer-based systems: "Assessing Reliability of Computer Output" (the little black book) and "Evaluating Internal Controls in Computer-Based Systems" (the big black book). The first is intended for independent use by generalist evaluators; the second, for generalists with TAG assistance. (The second requires significant audit experience with computer-based systems.)

#### Assessing output reliability

Although the little black book is an excellent guide for assessing the reliability of computer output, our study results indicate that, for several reasons, generalist evaluators do not use it. First of all, they believe it is too complex--that it requires more ADP knowledge and experience than most generalists have. Secondly, its use takes considerable time. We believe that, on the average, it would take a generalist about 30 staff-days to credibly assess the reliability of data generated by a simple computer-based system. Additionally, the little black book requires several judgments on the degree of risk involved in using information that may be inaccurate. Because they lack ADP knowledge and experience, most generalists feel uncomfortable making such judgments.

Although generalists do not use the little black book, they do assess output reliability by using traditional audit methods (many of which are described in the book). For example, they may trace computer outputs to the source documents, manually compute the source data, and compare their computations to the computer outputs. However, they often need assistance from TAG specialists to perform certain reliability tests (e.g., sophisticated statistical sampling). While generalists rarely hesitate to request such assistance, many are concerned that they may not always recognize instances when it is needed.

#### Evaluating internal controls

Like the little black book, the big black book ("Evaluating Internal Controls in Computer-Based Systems") is an excellent audit guide. However, several factors also limit its use. First, it is too complex. Because certain tests and procedures contained in the book are beyond the capabilities of the generalist, effective use of the book requires extensive assistance from TAG specialists. Additionally, its use takes considerable time. We believe that, on the average, it would take a generalist with ADP expertise over 180 staffdays to credibly review a simple computer-based system's internal controls.

Furthermore, applicability of the big black book to large, complex systems is limited. In our audit of DOE operations in the Albuquerque/Los Alamos area, for example, we were faced with a complex of 50 computer systems with more than 1,000 computerized programs. To give complete assurance, the big black book's audit steps would have had to be applied to each individual system, thereby multiplying the number of steps to be done and the corresponding time required to do them. Instead, we had to determine which of the book's audit steps most benefited the review, and apply only those. While this situation may be the exception today, the trend toward larger and more sophisticated computerized systems will likely make it the rule in the future.

How can cost-effectiveness  
be determined?

Because adequate application of either the little or the big black book requires considerable time, the corresponding cost is also considerable. Thus, it is both logical and cost-effective to determine the necessity and feasibility of performing either a full-scale internal control review or a computer output reliability assessment before committing the corresponding audit resources. We believe that this necessity and feasibility can be determined by analyzing information gathered about the computer-based system in question.

What assurance exists that  
sufficient data is gathered?

Data gathering, the key to any audit work, is the foundation of both the little and the big black books. To assist the staff in gathering sufficient and appropriate information on the computer-based system in question, both books contain detailed data-gathering steps and procedures. By analyzing the information gathered, the necessity and feasibility of assessing output reliability or internal controls can be determined, and the type and extent of audit work needed can be estimated.

For example, once the information specified by the little black book has been gathered, analysis of the information may indicate that

- further audit work is unnecessary or infeasible;
- a few simple, traditional audit tests will suffice; or
- a full-scale review of internal controls is warranted.

Similarly, analysis of data gathered through use of the big black book can indicate the necessity and feasibility of proceeding through the book, and the extent of audit work needed to complete an effective evaluation of internal controls.

However, because the little and big black books are rarely used, no assurance exists that sufficient and appropriate information is gathered on computer-based systems. Without this information,

- the need for an output reliability assessment or an internal control review may not be recognized or
- a time-consuming, costly reliability assessment or internal control review may be performed unnecessarily.

Therefore, management needs to assure that enough data is gathered on computer-based systems to facilitate decisions on the audit work needed.

**Who should analyze data gathered on computer-based systems to determine the related audit work needed?**

Most generalists are confident of their data-gathering capabilities. However, lacking extensive ADP knowledge and experience, they may not be able to independently analyze the data gathered on a computer-based system to determine the type and extent of subsequent audit work necessary. Thus, generalists usually need data analysis assistance from generalists with ADP expertise or TAG specialists. Additionally, since determinations of the type and extent of computer-related audit work needed involve resource application decisions (e.g., programing and staffing decisions), management should also be involved.

**COMPUTER-RELATED AUDIT WORK MUST BE DOCUMENTED**

Only with appropriate documentation can management assure that GAO standards and policy regarding computer-related audit work are met. Regardless of the type and extent of computer-related audit work performed, according to GAO audit standards and policy, the work methods and results must be documented. For example, an internal control evaluation, whether performed according to the big black book or not, should result in either a positive or a negative statement on the adequacy of controls. Similarly, an output reliability assessment, whether by the little black book or not, should result in a positive or a negative statement on the output's reliability. Whether or not GAO's audit guides are used, the methods employed to assess output reliability or internal controls should be documented, as should any scope or methodology limitations and any resulting effects. If it is deemed infeasible to assess the output reliability or the internal controls of a computer-based system involved in the review, a statement justifying that decision should be prepared.

Not only is documentation required by GAO policy, it also comprises a valuable data bank which assists management in making resource application decisions on computer-related work. For example, documentation of an output reliability assessment may indicate the need for a full-fledged review of a computer-based system's internal controls. Information included in this documentation (e.g., system size and operations, magnitude and complexity of potential control deficiencies, etc.) will assist management in determining what resources to dedicate for the review. Such documentation will also assist managers in determining priorities for future work. Thus, adequate documentation of computer-related audit work and decisions enhances efficient and economical application of GAO resources.

**CONCLUSIONS**

To judge whether an output reliability assessment or an internal control review is needed or feasible, adequate information on the computer-based system must first be gathered. Generalists may not have the ADP expertise and experience needed to analyze the information gathered to determine the type and extent of computer-related audit work necessary. However, generalists with ADP expertise and TAG specialists, together with management, can make such determinations. Documentation of these determinations and their justifications can assist management in judiciously prioritizing and planning computer-related audit efforts in accordance with GAO standards and policy.



Therefore, we developed an approach by which we can assure that

- sufficient information on computer-based systems is gathered;
- the possible use of computer output in support of audit findings is identified;
- the type and extent of audit work needed is determined;
- the computer-related audit decisions, work methods, and results are documented; and
- GAO's computer-related audit standards and policies are met.

This approach consists of (1) a one-page computer data collection instrument and (2) a decisionmaking process by which management can most effectively and efficiently allocate resources for reviews involving computer-based systems.

#### Computer data collection instrument

This instrument is intended for use by the generalist evaluator, who should be able to administer it in about 5 staff days. Attachment I presents the instrument and brief explanations of its contents.

#### Decisionmaking process

In addition to being a useful data-gathering tool, the instrument should assist resource management decisionmaking. By analyzing the data gathered through use of the instrument, audit staff and management can determine the type and extent of computer-related audit work needed on the current assignment and/or in future work. For example, the gathered data may indicate that a full internal control review is needed. At the other extreme, the gathered data may indicate that no further audit work is necessary to evaluate internal controls. In such a case, the considerable number of staff days needed (about 180) to evaluate internal controls will have been saved. If the data indicates that an output reliability assessment is needed, much of the background work (data gathering) will have already been done, and the assessment could be completed in less than 30 staff-days. Additionally, the data's indications of severe potential problems in a system's internal controls or output reliability should assist managers in prioritizing and planning their computer-related audit efforts. Attachment II presents a flowchart and a narrative description of the suggested decisionmaking process.

The Denver Regional Office is currently testing this approach and is finding it to be both economical and effective. Our first test was on a review of a military pay system. By applying the data collection instrument, we found that

- over 120 changes had been made to the system since GAO approved it;
- the system's data base was inaccurate and incomplete;
- source documentation was not readily available; and
- the internal control directive and review plan required to be issued by March 31, 1982, in accordance with OMB Circular A-123, had not been completed.

Due primarily to resource and time constraints, the report on this review will contain a statement that it was infeasible to evaluate internal controls or to further assess output reliability. However, based on our analysis of the data gathered through use of the collection instrument, we are planning further work on this system.

We believe that the information and documents we will obtain through use of the data collection instrument will enable us to determine the type and extent of computer-related audit work necessary and feasible on the current assignment and/or in future work. Through the use of our approach, management can also assure that computer-related audit decisions, work methods, and results are properly supported and documented. Such documentation is necessary to assure our compliance with GAO's audit standards and policy. A description of our experience to date with the use of the Data Collection Instrument is included as appendix V.

#### RECOMMENDATION

Because we have found this approach to be of value in meeting our computer-related audit responsibilities, we recommend that all GAO regions, divisions, and offices consider its use.

#### ATTACHMENTS TO THIS REPORT

- I Computer data collection instrument and brief explanations of its purpose and utilization.
- II Flowchart and narrative description of the suggested decisionmaking process.
- III Excerpts of GAO's "Policy and Procedures Manual for Guidance of Federal Agencies (Title 2 - Accounting)."
- IV OMB Circular A-123.
- V Summary of DCI Application Experience

COMPUTER DATACOLLECTION INSTRUMENT

This instrument is to assist the generalist evaluator in gathering information about computer-based systems involved in GAO reviews. This information will assist management in determining if further analysis of the computer system or assessment of data reliability is necessary and feasible. The instrument, which can be administered in about 5 staff days, consists of 24 "yes/no" questions. Of course, in asking the questions, the generalist is expected to apply professional judgment and sound audit techniques. For example, if an agency official responds that the agency's internal audit staff recently evaluated the computer-based system's general controls, the evaluator would be expected to request and review a copy of the resulting report. Following the data collection instrument are brief explanations of each question.

QUESTIONYES NO

1. Will computerized data be used to support findings? \_\_\_\_\_
2. Does the agency have a resident internal audit staff? \_\_\_\_\_
3. Is there an active, resident ADP planning group? \_\_\_\_\_
4. Has there been a recent evaluation of general controls? \_\_\_\_\_
5. Has there been a recent analysis of ADP application controls? \_\_\_\_\_
6. Does the system contain controls or data elements that are required by statute or regulation? \_\_\_\_\_
7. Is there a procedure to detect and follow up on any violations of such regulatory requirements? \_\_\_\_\_
8. Is a listing available of all computer equipment owned or leased? \_\_\_\_\_
9. Are lines of authority properly identified to assure adequate separation of organizational duties? \_\_\_\_\_
10. Is there adequate separation of responsibilities in data processing? \_\_\_\_\_
11. Does the system's current operation match design objectives? \_\_\_\_\_
12. Have there been recent changes to the data processing system? \_\_\_\_\_
13. Is software maintenance performed by agency personnel? \_\_\_\_\_
14. If software maintenance is contracted, does the vendor produce periodic status and test reports? \_\_\_\_\_
15. Is a computer security policy statement available? \_\_\_\_\_
16. Are stored data (tapes, disks, cards, etc.) protected? \_\_\_\_\_
17. Is system continuity protected by back-up power or another computer? \_\_\_\_\_
18. Is the computer system itself relatively simple? \_\_\_\_\_
19. Does the agency periodically test the reliability of computer output for timeliness, accuracy, and completeness? \_\_\_\_\_
20. Do users feel that data are timely, accurate, and complete? \_\_\_\_\_
21. Is adequate system documentation available? \_\_\_\_\_
22. Is there an up-to-date system user's manual? \_\_\_\_\_
23. Are hard copies of source documentation available? \_\_\_\_\_
24. Are all data base transactions properly authorized? \_\_\_\_\_

\*\*\*\*\*

Questions should be asked as follows:

Management: All questions except number 1.

ADP staff: All questions except numbers 1, 2, 4, and 20.

Users: Questions 6, 7, 9, 11, 12, 15, 16, 19, 20, 22, 23, and 24.

1. Will computerized data be used to support findings?

If the answer is "yes" or "don't know" for this one, the remainder of the questions should be administered. Even if the answer is "no," and you have time, a brief review may be of value for our permanent files.

2. Does the agency have a resident internal audit staff?

OMB Circular A-123 (See att. IV) requires agencies to establish, maintain, and evaluate internal controls in their program and administrative activities. Lack of an internal audit staff may indicate problems in the agency's compliance with the circular.

3. Is there an active, resident ADP planning group?

Since one of the vital aspects of a computerized system is its responsiveness to user requirements, the lack of such a group may indicate a lack of adequate planning and review procedures.

4. Has there been a recent evaluation of general controls?

If internal audit staff (or another audit organization) have recently evaluated general system controls and found them to be effective, further evaluation by GAO may be duplicative. If there has been such a study, the evaluator should attempt to judge its adequacy.

5. Has there been a recent analysis of ADP application controls?

Again, if agency personnel, or others, have performed such an analysis recently, further efforts on our part may be duplicative. However, as in No. 4 above, the evaluator should determine the adequacy of such work.

6. Does the system contain controls or data elements that are required by statute or regulation?

Some data systems are required by law to protect or to limit access to certain information. It is vital that the existence and effectiveness of such mandated controls or data elements be evaluated.

7. Is there a procedure to detect and follow up on any violations of such regulatory requirements?

If such a procedure is not set forth in writing and used, a serious problem may exist with internal controls. In this instance, depending on the size of the system, a detailed review may have to be conducted as a separate job.

8. Is a listing available of all computer equipment owned or leased?

This list will give the evaluator a perspective of the size and complexity of the agency's data processing activities. This, coupled with the data flow documents, will indicate how many systems could impact the data being analyzed. If there are many systems coming together to produce the data we will use, a full review of output reliability or internal controls may not be feasible in the time allotted for the job.

9. Are lines of authority properly identified to assure adequate separation of organizational duties?

The agency should have documented lines of authority that show each function's responsibilities. Checks, balances, and adequate review functions should be built into the system. Example: If the agency personnel who write checks are responsible for authorizing payments and entering transactions into the system, general controls are poor, indicating the need for an in-depth internal control review.

10. Is there adequate separation of responsibilities in data processing?

Programers, analysts, system managers, operators, etc., should be denied uncontrolled access to production program files, production data files, terminal entry capabilities, and operating system software where control over transmission and execution modes is maintained. Console operators should be prohibited from modifying programs. Additionally, operators of input preparation equipment should be prohibited from altering data on source documents and should be denied access to computer programs.

11. Does the system's current operation meet design objectives?

If the system is not doing what it was intended to do, this may indicate inadequate planning or testing, problems in contracting procedures and contract management, or poor overall program management.

12. Have there been recent changes to the data processing system?

If such changes were made to correct previously identified system weaknesses, and testing has shown them to be effective, further work by GAO may be duplicative. On the other hand, a quick check on what the changes were supposed to do, and what they actually accomplished, could indicate further audit needs. Also, some changes to accounting and financial management systems are subject to GAO approval.

13. Is software maintenance performed by agency personnel?

If so, documentation needed to perform an internal control evaluation or an output reliability assessment should be readily available.

14. If software maintenance is contracted, does the vendor produce periodic status and test reports?

In most software maintenance contracts, periodic reviews of system reliability are required. In any case, system documentation is always required. The resulting reports, if adequate, could meet our requirements for assessing the system's controls or output data reliability.

15. Is a computer security policy statement available?

Such a statement is usually contained in a security procedures manual or a user's manual. If the agency has articulated its security procedures, review of internal controls will be facilitated. If not, extra work may be required to determine why and how controls are structured in the system.

16. Are stored data (tapes, disks, cards, etc.) protected?

Since computerized data represents a valuable asset (i.e., it would cost resources to replace it), such data should be afforded adequate protection. Lack of protection could cause the catastrophic loss of data.

17. Is system continuity protected by back-up power or another computer?

Any well-designed system should adequately consider contingencies such as computer or power failure either damaging or totally destroying valuable data. If such a back-up capability does not exist, this could be the subject of a separate report, depending on the severity of possible data loss and its impact on agency operations.

18. Is the computer complex itself relatively simple?

This is a subjective judgement that can best be made after talking to the agency's ADP staff. A "simple system" has one set of data inputs, one processor, and one set of outputs. An example of this would be a simple payroll system. A complex system, on the other hand, has many data bases, many computers and data entry devices (terminals), and it may be internettted to another computer system. The outputs may never be printed out; they may be "dumped" to a summary tape and sent elsewhere. On a simple system, a reliability assessment takes about 30 staff days, and an internal control evaluation, about 180 staff-days. On a complex system, proportionally more time is needed.

19. Does the agency periodically test the reliability of computer output for timeliness, accuracy, and completeness?

If the agency periodically performs adequate testing, this could obviate further reliability assessment on our part. The key here is the adequacy of such tests.

20. Do users feel data are timely, accurate, and complete?

Although users often have limited knowledge of computer processing capabilities and requirements, many times their general observations and casual assessments may indicate serious computer problems. However, if the users all agree that the data are timely, accurate, and complete, this may limit further assessment on our part.

21. Is adequate system documentation available?

Such documentation is needed for an agency's use in operating the system and for any meaningful audit of the system. It is also required by GAO's "Policy and Procedures Manual for Guidance of Federal Agencies (Title 2 - Accounting)." See attachment III for a detailed listing of the documentation required for computer-based systems.

22. Is there an up-to-date system user's manual?

The user's manual will give the evaluator an idea of what data sources are used, how and when data are processed, and what reported data are available. This document should be up to date and readily available. If not, output reliability assessment will be difficult and time consuming.

23. Are hard copies of source documentation available?

In any audit, we generally trace summary and reported data to originating documents as a test of output reliability. If such documents are not readily available, it will be more difficult and require more time to conduct a meaningful assessment of output reliability or evaluate internal controls.

24. Are all data base transactions properly authorized?

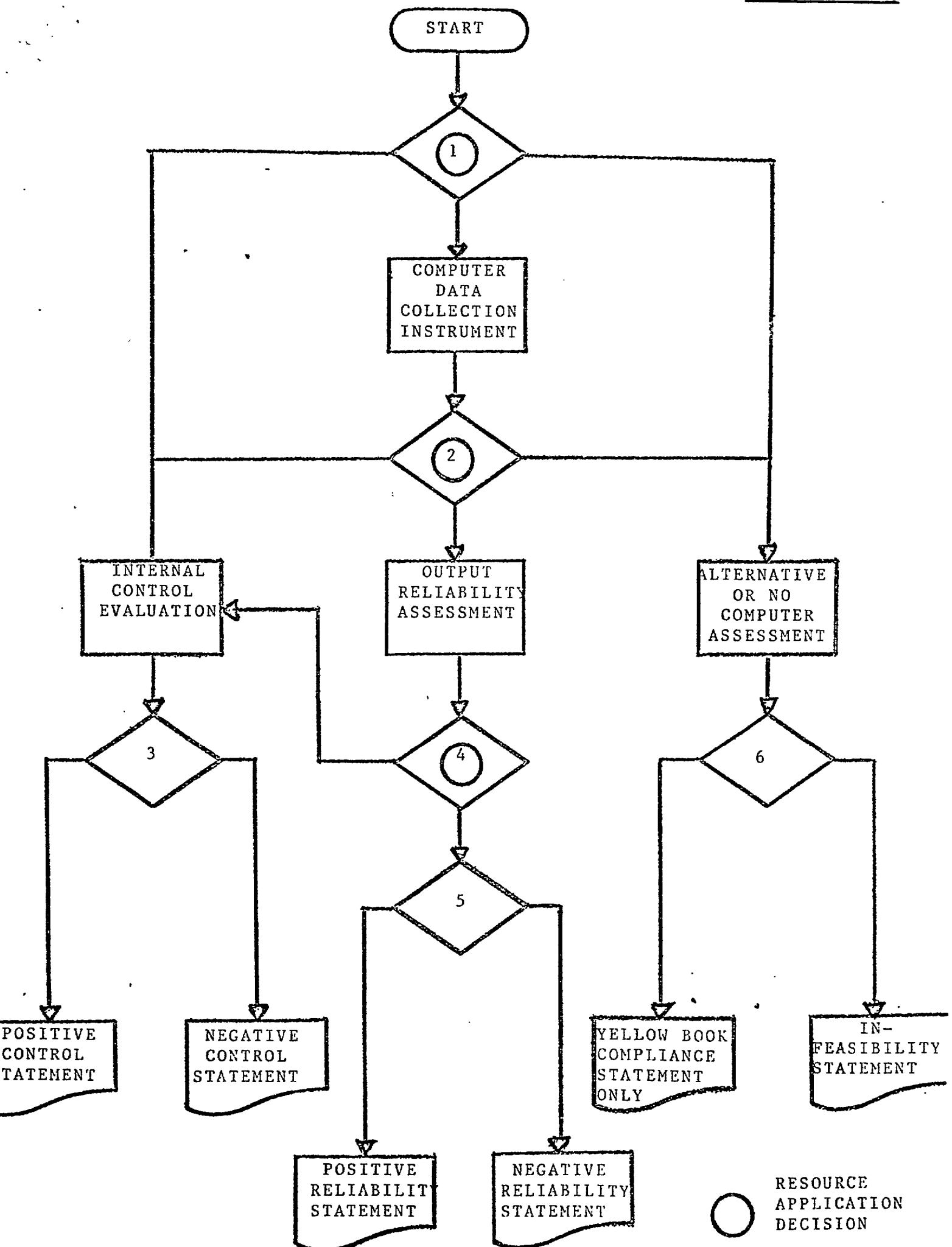
Lack of well-defined, controlled, access to data files may indicate serious system deficiencies and the need for more detailed review of internal controls.



DECISIONMAKING PROCESSFOR COMPUTER-RELATED AUDIT WORK

The following decisionmaking process should assist management in determining the most efficient and cost-effective application of resources on assignments involving computer-based systems. We believe this process provides a logical approach to assuring that the appropriate type and extent of audit work is determined, done, and documented on reviews involving computer-based systems.

Following are a flowchart and a narrative explanation of the suggested decisionmaking process.



EXPLANATION OFDECISIONMAKING FLOWCHART

Decision point number one on the flowchart is the point at which a job is programmed. Three decision paths branch from this point, and which path is chosen will depend on the type and extent of existing information. For example, if previous survey work has demonstrated the need for an internal control evaluation of a computer-based system, the left-hand path will be chosen, and an internal control review will be programmed. If, however, existing information indicates that an internal control evaluation and a computer output reliability assessment are either unnecessary or infeasible at the current time, the right-hand path will be chosen, and neither type of assessment will be performed during the programmed assignment.

The right-hand path might be chosen, for example, when a system's internal controls have recently been evaluated, and the evaluation resulted in a positive control statement, or when a recent output reliability assessment resulted in positive findings. Various other factors might also dictate choice of this path. For example, computer-processed information may not be relevant to the review objectives; information necessary to assess output reliability may not exist; or the time required to assess output reliability (about 30 staff days) or internal controls (about 180 staff-days) may preclude such audit work on the current assignment.

In most cases, sufficient information will not exist to justify choosing either the left- or right-hand path at decision point number one. In these cases, the center path will be chosen, and the computer data collection instrument (DCI) will be used (requiring about 5 staff-days) to gather information necessary for decision point number two. From the information and documents gathered through use of the instrument, a decision may be made on the type and extent of further audit work necessary to evaluate internal controls or to assess output reliability.

Decision point number two is the point at which analysis of the information gathered will determine the type and extent of audit work needed on the job (and on future jobs). Again, three paths branch from this decision point. If the information indicates the need for an internal control review, the left-hand path will be chosen, and the job will be expanded (or another programed) to include an internal control (big black book) evaluation. Following implementation of the internal control evaluation, decision point number three will be reached.

Decision point number three is the point at which analysis of the review's findings will dictate either a positive or a negative statement on the internal controls. Examples of both statements follow. (In most of our reviews, of course, the findings will not be all positive or all negative, but rather a mix of the two.) Thus, the following examples are intended only as guidelines; the language of the actual statement will vary from job to job.)

POSITIVE CONTROL STATEMENT

"We performed our review in accordance with GAO's 'Standards For Audit of Governmental Organizations, Programs, Activities, and Functions.' Generally, we found that the internal controls of the agency's computer-based system(s) were designed according to management direction and operating effectively. Data processing appears timely, accurate, and complete. We found no deficiencies that warrant further review at this time."

NEGATIVE CONTROL STATEMENT

"We performed our review in accordance with GAO's 'Standards For Audit of Governmental Organizations, Programs, Activities, and Functions.' We found the internal controls in the agency's computer-based system(s) to be generally inadequate to assure timely, accurate, and complete processing of data. Specific findings in this area are included in chapter \_\_\_ of this report. Our recommendations for further computer audit efforts are included in chapter \_\_\_."

If, however, at decision point number two, the information gathered through use of the data collection instrument indicates the need for an output reliability assessment, the center path will be chosen, and a little black book assessment will be performed. Decision point number four is the point at which analysis of the assessment will dictate either branching off to an internal control evaluation or proceeding to decision point number five. At this point, depending on the assessment results, either a positive or a negative output reliability statement will be prepared. Examples of both statements follow, again, as general guidelines.

POSITIVE RELIABILITY STATEMENT

"Although we performed our review in accordance with GAO's 'Standards For Audit of Governmental Organizations, Programs, Activities, and Functions,' we did not fully evaluate the computer-based system's internal controls because of (list applicable reasons, e.g., time and/or resource constraints). We did, however, assess the reliability of computer-generated data used as support for findings disclosed in this report. We found no instances of erroneous data and no issues that warrant further review of the agency's computer system."

NEGATIVE RELIABILITY STATEMENT

"Although we performed our review in accordance with GAO's 'Standards For Audit of Governmental Organizations, Programs, Activities, and Functions,' we did not fully evaluate the computer-based system's internal controls because of (list applicable reasons). We did, however, assess the reliability of computer-generated data used as support for findings disclosed in this report. We found several deficiencies that caused us to question the overall accuracy of computer output. The audit methods we used, and the deficiencies found, are discussed in chapter \_\_\_."

In other instances, the information gathered from the data collection instrument (at decision point number two) will indicate that a detailed reliability assessment and an internal control review are either unnecessary or infeasible at the time. If computer-based systems are not involved in the review, the resulting statement will be one of compliance with GAO audit standards.

YELLOW BOOK COMPLIANCE STATEMENT

"We performed our review in accordance with GAO's "Standards For Audit of Governmental Organizations, Programs, Activities, and Functions."

If, however, it is deemed infeasible to assess internal controls and output reliability, justification for that decision will be prepared, and a statement of infeasibility will result. An example follows.

INFEASIBILITY STATEMENT

"We performed our review in accordance with GAO's "Standards For Audit of Governmental Organizations, Programs, Activities, and Functions." Because of (list applicable reasons, e.g., system complexity, number of computer systems involved, availability of alternative methods, prohibitive cost of such review, and/or time constraints), we did not assess data reliability or evaluate internal controls in the computer-based system(s). As a result, (list any resulting effects, limitations, or qualifications)."

POLICY AND PROCEDURES MANUAL  
FOR GUIDANCE OF FEDERAL AGENCIES

TITLE 2 -- ACCOUNTING

Section 27.5 General System Design § 1 thru 8

27.5 GENERAL SYSTEM DESIGN

System design presentations to the Comptroller General for approval should consist of a concise but comprehensive exposition, by combination of description, chart, diagram, and example, of all of the essential elements of the system design. The term "general system design," as applied to accounting systems, excludes detail of procedures and instructions for use by employees in operating an accounting system.

The design presentation should demonstrate that the system, in all of its essential elements, conforms to the agency's approved principles and standards and should include the items listed below. (Each item should be considered as invoking all of the principles and standards pertinent to it and as requiring demonstration that it is appropriately applied to the entity involved.)

1. A general description of the accounting system
  - a. The overall design concept of the accounting system.
  - b. The relationship of the accounting system to:
    - (1) The agency's program, budget, and organizational structure.
    - (2) The missions, functions, and financial management needs of the entity.
    - (3) The agency's total management information system.
  - c. A summary of the classification coding to be used.

- d. The interface of the accounting system with other accounting systems in operation or under development in the agency.

2. The financial reports to be produced

- a. A description, supported by a chart, of the overall recurrent reporting plan of the entity (e.g., pyramidal reporting) in regard to:
  - (1) Its internal operations, including lower management echelons.
  - (2) External reporting responsibilities.
- b. A listing by title (and form number, if assigned) of recurring internal reports prescribed by the system, including for each report the frequency and the period covered, or "as of" dates.
- c. Each recurring internal report prescribed by the system should include:
  - (1) The types of financial information to be provided to the various levels of management.
  - (2) A sample of the format showing illustrative data elements (columnar headings and stub captions), with pro forma data inserted.
- d. A listing by title and form number of external reports to be produced by the system.

3. The accounting records to be maintained

- a. A listing of the general ledger accounts by title and number.
- b. A definition of each general ledger account, including the intended account content, control functions in respect to subsidiary ledgers, and identification of each affected account.
- c. A listing or an outline of the subsidiary accounts to be maintained.
- d. A description of the books of original entry (transaction files in the case of ADP applications) and

their functions in regard to the agency's general ledger and subsidiary account structure.

- e. A description of the locations and organizational levels at which accounts and supporting documentation will be maintained and at which accounting activities will be performed.

4. The major accounting processes

- a. Charts depicting the flow of documentary data through the principal accounting processes, supplemented by sufficient description to enable relating the actions charted to the accounting objectives, records, internal controls, and financial reporting requirements included in the design presentation.
- b. An explanation of methods to be used in determining and recording the amounts of and the accounting for accrued expenditures, revenues, and costs.

5. Accounting for costs

A description of the manner in which costs are accounted for in accordance with section 16, in regard to each functional area, including:

- a. The role of cost accounting, in terms of resources consumed (whether funded or unfunded), in relation to the program and operation.
- b. The degree of refinement of operational classifications for cost accounting purposes.
- c. The rationale and criteria by which accrued expenditures for personal services, materials and supplies, equipment, and other purposes will be charged as costs in the operational classifications.
- d. The role of cost centers or other accounts for allocating, charging, and accumulating costs.
- e. An explanation of the coding structure used as a basis for distributing and summarizing costs by activity.
- f. The extent of association of quantitative data with costs.



- g. The relationship of the cost accounts to the agency's cost-based budgeting.
- h. Whether all or only significant elements of cost are included and, if the latter:
  - (a) What elements of funded and unfunded cost will be included and excluded.
  - (b) Whether distinction will be made between controllable and uncontrollable costs.
- i. The areas where cost-finding techniques will be used in lieu of cost accounts.

6. The extent and nature of mechanization and automation

In a system employing ADP equipment, adequate documentation varies according to the circumstances involved but is necessary for the success of any operation. The types of documentation specified below are deemed necessary to provide an understanding of the design of the system and to enable an evaluation of the adequacy of system controls and audit trails. Programmed instructions and operator instructions are not required to be submitted.

Required documentation includes:

- a. The planned use of ADP and other mechanical equipment, including the following.
  - (1) A statement of objectives for the use of automation and for the degree to which the system will be automated.
  - (2) An overall narrative description and accompanying flowchart of the general flow of information through the system. This should tie in with the general description of the accounting system.
  - (3) A description of the equipment configuration and capabilities, and the computer language(s) which will be utilized in programming the processing operations. When specific equipment has not been selected, the description should include a statement of the general equipment requirements for processing, storage, and associated

peripheral operations, and a statement of the primary computer language to be used.

b. The design specifications which describe the logic of the proposed ADP system, including:

- (1) Flow charts showing the sequence of operations to be performed by each proposed computer process.
- (2) For each proposed computer program, a brief description of the functions to be performed, processing frequency, type of input, and the resulting product(s).
- (3) Descriptions of the physical characteristics of the data elements to be contained in the transaction records and data files, including the media (punched card, magnetic tape, etc.) to be used.
- (4) Descriptions of controls to be provided over data:
  - (a) Inputs, including the types and purposes of edit and other purification or validation routines.
  - (b) Processing, including the plan for backup operations.
  - (c) Storage, including the plans for reconstruction of the data files.
  - (d) Outputs.
- (5) Identification of audit trails in the automated system with special attention given to systems in which conventional audit trails (see item 7 below) will be obscured in the processing operations and alternative procedures will be necessary.

7. The internal controls to be maintained

- a. A description of the manner in which financial, manpower, and property resources are controlled and safeguarded by the regular authorization, ap-

proval, documentation, recording, reconciling, reporting, and related accounting processes.

- b. An outline of controls over quantity, timeliness, reliability, and accuracy of inputs, processing, and outputs (whether for manual, automated, or mechanical systems), sufficient to demonstrate reasonable assurance of accurate recording of transactions and reporting of their effects in the accounting period in which they occur.
- c. A statement of the basis for auditability of the system in terms of results of operation and current condition, and identification of the audit trails throughout the system. This includes a description of the manner in which a particular element of data existing in the files can be traced backward to its source and forward to its position in a report.

8. The plans for implementing the accounting system

- a. The proposed conversion process, including plans for training and a tentative schedule for implementation.
- b. A brief description of the planned methods for testing the logic and reliability of the system.



EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF MANAGEMENT AND BUDGET

APPENDIX IV

WASHINGTON, D.C. 20503

October 28, 1981

CIRCULAR No. A-123

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Internal Control Systems

1. Purpose. This Circular prescribes policies and standards to be followed by executive departments and agencies in establishing and maintaining internal controls in their program and administrative activities.
2. Background. The Budget and Accounting Procedures Act of 1950 requires the head of each department and agency to establish and maintain adequate systems of internal control. The Antideficiency Act, 31 U.S.C. 665, requires that agency systems for the control of funds be approved by the Director of OMB. Despite these statutory requirements, there continue to be numerous instances of fraud, waste, and abuse of Government resources and of mismanagement of Government programs. These problems frequently result from weaknesses in internal controls or from breakdowns in compliance with internal controls.
3. Policy. Agencies shall maintain effective systems of accounting and administrative control. All levels of management shall involve themselves in assuring the adequacy of controls. New programs shall be designed so as to incorporate effective systems of internal control. All systems shall be evaluated on an ongoing basis.
4. Definitions. For the purpose of this Circular, the following terms are defined:
  - a. Agency -- any department or independent establishment of the executive branch.
  - b. Agency Component -- a major organization, program, or functional subdivision of an agency having one or more separate systems of internal control.
  - c. Internal Controls -- the plan of organization and all of the methods and measures adopted within an agency to safeguard its resources, assure the accuracy and reliability of its information, assure adherence to applicable laws, regulations and policies, and promote operational economy and efficiency.

d. Internal Control Documentation -- written policies, organization charts, procedural write-ups, manuals, memoranda, flow charts, decision tables, completed questionnaires, software, and related written materials used to describe the internal control methods and measures, to communicate responsibilities and authorities for operating such methods and measures, and to serve as a reference for persons reviewing the internal controls and their functioning.

e. Internal Control System -- the totality of the methods and measures of internal control for all or part of an agency.

f. Vulnerability Assessment -- a review of the susceptibility of an agency or program to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and/or adverse or unfavorable public opinion.

g. Internal Control Review -- a detailed examination of an agency's or agency component's system of internal control to determine whether adequate control measures exist and are implemented to prevent or detect the occurrence of potential risks in a cost effective manner.

5. Responsibility. Designing, installing and monitoring internal control systems for their effectiveness and identifying and initiating needed changes is the responsibility of the agency head. The Inspector General, or his equivalent in agencies without an Inspector General, also has a responsibility in regard to internal controls, as explained in paragraph 5b.

a. Agency heads are responsible for the establishment and maintenance of a system or systems of internal control within their agencies. This responsibility includes determining that the system is functioning as prescribed and is modified, as appropriate, for changes in conditions.

Each agency head shall issue an internal control directive (if one does not exist) and a review plan by March 31, 1982 (see paragraph 8). Where additional internal control directives are required for agency components, the head of the agency shall ensure that such directives are consistent with the agency directive.

b. The Inspector General, or the senior audit official where there is no Inspector General, will, in conjunction with internal audits, review internal control documentation, systems, and compliance to determine whether the policies and standards established by this Circular are being implemented properly. Reviews should also be made of the audit follow-up system in order to ensure management's follow-up of audit findings and recommendations. Additional reviews will be performed as necessary to provide sufficient agency coverage.

6. Objectives of Internal Control. The objectives of internal control are to provide management with reasonable, but not absolute, assurance that financial and other resources are safeguarded from unauthorized use or disposition; transactions are executed in accordance with authorizations; financial and statistical records and reports are reliable; applicable laws, regulations and policies are adhered to; and resources are efficiently and effectively managed.
7. Standards of Internal Control. Certain basic standards shall be adhered to in the system(s) of internal control established by an agency, or agency component. These include:
  - a. Documentation -- Internal controls, accountability for resources, and all financial transactions shall be clearly documented, and documentation shall readily be available.
  - b. Recording of Transactions -- Transactions shall be recorded as executed, when executed, and be properly classified.
  - c. Execution of Transactions -- Independent evidence shall be maintained that authorizations are issued by persons acting within the scope of their authority and that transactions conform with the terms of the authorizations.
  - d. Separation of Duties -- Key duties such as authorizing, approving, recording transactions, issuing or receiving assets, making payments, and reviewing or auditing shall be assigned to separate individuals to minimize the risk of loss to the Government. Internal control depends largely on the elimination of opportunities to conceal errors or irregularities. This in turn depends on the assignment of work in such a fashion that no one individual controls all phases of an activity or transaction, thereby creating a situation that permits error or irregularities to go undetected.
  - e. Supervision -- Qualified and continuous supervision shall be provided to assure that approved procedures are followed. Lines of personal responsibility and accountability shall be clear.
  - f. Access to Resources -- Access to resources shall be limited to authorized personnel. Access includes both direct physical access and indirect access through the preparation or processing of documents that authorize the use or disposition of resources. Periodic comparison shall be made of the

resources with the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

g. Competent Personnel -- Reasonable care shall be taken that key personnel have high standards of integrity, and are competent, by education, training or experience to accomplish their assigned duties.

h. Reasonable Assurance -- Internal control systems shall provide reasonable, but not absolute, assurance that the objectives of the system will be accomplished. This standard recognizes that the cost of internal controls should not exceed the benefits derived therefrom, and that the benefits consist of reductions in the risks of failing to achieve the stated objectives.

8. Requirements for Agency Internal Control Directive and Plans.  
An agency directive and accompanying plan required by paragraph 5 will, at a minimum:

a. Identify an appropriate official, establish an internal control committee, or otherwise establish specific responsibility for seeing that agency internal control systems are developed (where they do not exist), maintained, reviewed, and improved as necessary.

b. Provide for coordination between program managers and technical staffs, including the Office of Inspector General or its equivalent in agencies without an Inspector General, in matters concerning internal control.

c. Assign responsibility for internal control to specific officials in each component of the agency and provide that performance appraisals reflect accomplishments of this responsibility.

d. Require each internal control system to meet the standards of internal control described in paragraph 7.

e. Provide a plan by March 31, 1982 for vulnerability assessments covering all agency components to be accomplished by December 31, 1982, and as frequently as circumstances warrant thereafter, but not less frequently than biennially. Such assessments should be used to determine when and in what sequence reviews of the effectiveness of internal controls should be performed and systems improved or documented.

Vulnerability assessments should consider, but need not be limited to, the following: newness of the program, dollar value of the program, nature of the program and its clientele, recent changes in program control or resource levels, impact of the program on persons or organizations external to the agency, the appreciation for effective internal control by

persons operating the program, assumed effectiveness of existing controls, recent instances of errors or irregularities, and the interval since the most recent evaluation or audit.

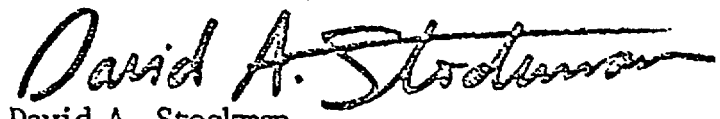
f. Provide for internal control reviews on an ongoing basis to determine whether the controls are operating as intended and are effective. These reviews should identify internal controls that need to be strengthened or streamlined. They should be a part of normal management and budget analyses and should draw on available audit reports and other sources.

The frequency of the reviews shall be determined by the Inspector General and/or the agency head. The Inspector General may do a review at any time.

g. Establish administrative procedures to enforce the intended functioning of the internal controls. Included in the procedures should be notations in performance appraisals for positive accomplishments related to internal controls, appropriate disciplinary actions for violations of internal controls, and correction of internal control weaknesses, however identified.

These procedures should also include reports to the agency head on all significant internal control breakdowns and financial losses, in accordance with criteria established by the agency head. Reporting and discipline for lesser violations may be handled at lower levels.

9. Specific Internal Control Guides. Models and other guidelines for internal controls for specialized aspects of agency operations will be developed from time-to-time and issued separately to aid agencies in designing specific internal control systems.
10. Reporting. Agencies may be required to include information on financial losses, system breakdowns and progress in making system reviews as part of their annual report to OMB on financial management improvement.
11. Effective Date. This Circular is effective on publication.
12. Inquiries. All questions or inquiries should be addressed to the Financial Management Branch, Office of Management and Budget, telephone number 202/395-4773.
13. Sunset Review Date. This Circular shall have an independent policy review to ascertain its effectiveness three years from the date of issuance.



David A. Stockman  
Director



Application Experience

Since March 1982, we have been testing the Denver Approach to auditing computer-based systems in the Denver Region. Special emphasis has been given to applying the Data Collection Instrument (DCI) to jobs where it was determined that computer-based information was involved in supporting our findings and conclusions. To date, we have applied the DCI to 16 audits in the Denver Region.

For seven of those 16, the application was limited, either because computerized data was not used to support findings (1), the job was terminated (1), the scope was changed (2), the job itself was a review of accounting controls (2), or the job scope precluded use of the check list at this time (1). The following is a specific listing of the jobs on which the DCI has been applied, and the results obtained in each case:

1. Job Code 005274 - Western Area Power Administration

Application of the DCI indicated that while general and applications controls existed, they were not effective (or utilized). Further work will be suggested in this area.

2. Job Code 008508 - Controls Over Minerals Lease Rent

DCI application surfaced problems in both general and application controls. Further work planned for future.

3. Job Code 008509 - Oil and Gas Lottery Issues

Application of DCI disclose significant control problems, general and application, that warrant review. Work is being planned in this area.

4. Job Code 009721 - Survey of EDIS' Information Centers

Job is currently in survey stages. Checklist will not be utilized until it is determined which of the computer systems outputs will be used to support findings.

5. Job Code 016001 - Information Technology Improvements

This job was basically concerned with the use of micrographics technology and utilization. Computerized data output, per se was not used.

6. Job Code 101046 - DOD Enrollment Eligibility Systems

An alternative to black book assessments was deemed to be more effective due to time and resource constraints. Source documents were used to audit around the computer system. General controls were found to be questionable. Further work is planned for that area.

7. Job Code 300552 - Department of Energy Task Force

This review was basically general controls. Information on application controls was provided to staff performing Job Code 905064, which was a full internal control (big black book) audit.

8. Job Code 903044 - Review of Controls on Retired Pay

Application of the DCI resulted in the current review of Air Force Accounting and Finance Center computer systems, Code 903054.

9. Job Code 903049 - Foreign Sales Progress Payments

This job was terminated, therefore DCI was not completed.

10. Job Code 905064 - Department of Energy Task Force

This was a full scale internal control review. As pointed out in our report on the Denver Approach, it was performed utilizing portions of the big black book. The different aspects of the DCI were incorporated into the audit program. This review disclosed various general and application control problems.

11. Job Code 910352 - Productivity of Payroll Systems

In this survey, the staff is currently going to 31 locations. The application of the DCI has been postponed until the 3 or 4 systems that will be audited have been identified.

12. Job Code 913694 - Survey of Government ADP Resources

The DCI was incorporated into the audit program for this survey. It is being applied at every major computer installation in the Denver Region. To date, at least six major systems have been identified in the Denver Region for full scale control review.

13. Job Code 942136 - Civil Pricing Denver

This job is in the survey phase. The Check list is being applied as the opportunity presents itself. All agencies at which it will be applied have not been identified, and results to date have not been tabulated.

14. Job Code 951677 - Adequacy of Test Resources

The check list has been partially applied. This review is still in the survey phase, and the exact data on which reliability must be assessed have not yet been totally identified.

15. Job Code 966056 - Federal Overtime Practices

The application of the DCI was limited in this job, since it dealt basically with general controls (before information input to computer) on time cards and authorizations of overtime. Several computer system problems were noted, however, and forwarded to the Washington Programming Group for inclusion in future work.

16. Job Code 99703452 - Defense Logistics Agency's DWASP System

This job has been rescoped and now is current as Code 949038, with the purpose of preparing work proposals for the DWASP system. It is expected that the DCI will play a prominent role in the survey and review being planned at this time.

SUMMARY

We found that, even with limited testing, the potential utility of the DCI is significant. In every job where it has been fully applied, it has disclosed significant problems in the general and application controls of the system that probably would not have been surfaced otherwise. We intend to keep using the DCI, and have incorporated it into an overall check list for compliance with all the requirements of GAO's "Standards For Audit of Governmental Organizations, Programs, Activities, and Functions."

To date, the generalist evaluators have been able to apply the DCI, after a short explanation, with minimal technical assistance. We feel that the reason for this is its foundation being in basic auditing principles. For the purpose of assisting the generalist evaluator to gain some insight into the computerized systems he or she encounters, it appears well suited. It is our opinion that this DCI, or a similar document should be used on every job in GAO that has computer involvement prior to application of either of the black books. On those jobs where we have utilized the DCI, we are more confident of the timeliness, accuracy, and completeness of computerized data than we would have been by using traditional audit methods based on auditing around the computer.